Defense Health Agency (DHA) Privacy and Civil Liberties Office (PCLO) PIA Guide

*Please refer to the **italicized wording** for assistance*

Complete and submit DD Form 2930 to the DHA PCLO for review using dha.ncr.pcl.mbx.piamail@mail.mil. Please notify DHA PCLO should there be any system change that involves the collection of PII.

PRIVACY IMPACT ASSESSMENT (PIA)

For the

***Enter the name of the* DoD Information System/Electronic Collection Name**

(e.g., Information System (IS))

***Enter the* DoD Component Name**

Type "Defense Health Agency (DHA)"

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors. *See Page 2 (Section 1, c.) for further instructions.*

☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No. *See Page 2 (Section 1, b.) for further instructions.*

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

For those cases where a PIA is not required, proceed to Section 4; obtain the Program Manager and Program Level Senior Information Assurance Officer signatures. Send the signed form to the DHA PCLO.

If applicable, update DHP SIRT and/or DITPR to reflect a.) that no PII is collected and b.) a PIA is not required.

c. If "Yes," then a PIA is required. Proceed to Section 2.

If the PII collected is strictly internal government operations related (e.g., name, badge number, office phone, office e-mail, etc.) then no PIA is required. Please complete the following:

1.) Provide a system description and enter the following statement into Section 2(g)1 of this PIA:

> *"A PIA is not required per DoDI 5400.16 (Enclosure 3, 1(c)) because the PII is related to strictly internal government operations, does not include members of the public, and PII data is considered low or no risk."*

2.) Return the PIA to the DHA PCLO for review and approval.

3.) Upon review, the DHA PCLO Chief will advise whether a PIA is required.

4.) If applicable, update DHP SIRT and/or DITPR to reflect a.) that PII is collected but b.) a PIA is not required.

PIA Drafting Guidelines:

1. *Remember the audience. The PIA should be written in a manner that allows the public to understand the activities being described. The PIA should be written with sufficient detail to permit the DHA PCLO to analyze the privacy risks and mitigation steps.*
2. *Correct simple errors. Sections 1 and 2 of this document are meant to be published on the DHA PCLO web site. Any PIA submitted to this office should be free of spelling and grammatical errors and written in active voice rather than passive voice.*
3. *Explain Acronyms. Spell out each acronym the first time it is used in the document. For example: Office of Management and Budget (OMB).*
4. *Use Plain English. Use words, phrases, or names in the PIA that are readily known to the average person.*
5. *Define technical terms or references. Keep in mind that readers may not understand technical terms when they are first used.*
6. *Cite legal references and other previously published documents. Reference other projects and systems and provide explanations, for the general public to gain a complete understanding of the context of the program or system. If a document has previously been published in the Federal Register, for example a system of records notice, provide the citation, and if possible a very brief description of the document type (e.g., system of records notice, statute, final or proposed rule).*
7. *Use the complete name of reference documents. For example: National Institute of Science and Technology (NIST) SP 800-26, Security Self-Assessment Guide for Information Technology Systems. Subsequent references may use the abbreviated format.*

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☐ **New DoD Information System** ☐ **New Electronic Collection**

☐ **Existing DoD Information System** ☐ **Existing Electronic Collection**

☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

Your Program Manager will know whether or not your DoD Information System is registered in DITPR or SIPRNET. Only information systems that belong to the DoD (e.g., not contractor owned) will be registered.

☐ **Yes, DITPR** Enter DITPR System Identification Number

☐ **Yes, SIPRNET** Enter SIPRNET Identification Number

☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

Note: The UPI is now referred to as the Unique Investment Identifier (UII).

DoD Information systems that are owned and operated by third parties (i.e., contractor companies) may not have a UII. The system owner should be able to provide this number.

☐ **Yes** ☐ **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does the DoD information system or electronic collection have a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

A SORN is required if you answer "Yes" to each of the following questions:
1.) Does the system contain "records" as defined by the Privacy Act?
2.) Are the records in the system under the control of DoD or a DoD component?
3.) Are the records in the system retrieved by a name or other personally identifiable information (PII)?

If a SORN is necessary, you must initially determine whether an existing SORN applies to your system or that the system requires a new SORN. You should recommend which SORN you feel most closely aligns with the functionality and purpose of the system, based on the descriptions contained within each SORN (i.e., descriptions of categories of records in the system; categories of individuals covered by the system; authorities to collect; and routine uses of records maintained in the system, etc.). Current SORNs are available at the following link: http://www.tricare.mil/tma/privacy/RoleoftheTMAPrivacyOffice.aspx#sorn for your review. We are available to provide further assistance if needed. Once a preliminary SORN selection has been made, please provide the SORN identifier (e.g., DTMA 01) in the space provided below. The Privacy Act Team will review your preliminary selection and assist with final SORN determination and/or development of a new SORN, if necessary.

☐ **Yes** ☐ **No**

If "Yes", Enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number. Consult the Component Privacy Office for additional information or access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office

Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format. *If a form and/or system is being used to collect the data from other than DoD military (active or reserve), DoD Civilians, or other Federal employees, then OMB approval will be required. (Unless there is an exemption noted in an approved authority).*

If OMB approves the information collection requirements, it assigns a control number and expiration date. Please provide OMB Control Numbers and form numbers for all input and output forms (Standard Form (SF) or Department of Defense (DD)) produced by or used by the system. The OMB Control Number and expiration date are typically located in the upper right hand corner of approved forms.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☐ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provision of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute and/or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive or instruction implementing the statute within the DoD Component should be identified.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

Response should indicate:

- ✓ *the primary uses of the system/application (i.e., explain how the system uses PII (workflow process, include information about other pertinent system components));*
- ✓ *provide a general description of personal information about individuals that is collected in the system (e.g. personal descriptors, ID numbers, ethnicity, health, financial, employment, credit, criminal, life, and/or education) (note: the information must be provided in detail in Section 3a.(1);*
- ✓ *the specific categories of individuals (e.g. dependents, retirees and/or their dependents, active duty, contractors, foreign nationals, former spouses, reservist, national guard personnel) that information will be collected from (or about) within the system; and*
- ✓ *the office that owns and/or manages the IT system.*

Note: the length of this entry will depend on the size and complexity of the IT system (and its subsystems, where relevant).

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Response should indicate how you have identified and mitigated any privacy risks in the system / application (e.g., awareness and training programs, limited physical access, data encryption, violations for unauthorized monitoring, etc.) in order to sufficiently reduce system / application vulnerabilities to a reasonable and appropriate level. (Note: it is appropriate to address administrative, physical, and technical controls in place to protect the system (DoD 8580.02-R, DoD Health Information Security Regulation, C2 – C4).)

Please do not provide specific information about the name / vendor / operating system of any security measures you identify; if made publically available, this information could be used to maliciously attack the IT system / application.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

If your system / application shares data with another system / application, include that system under the appropriate sub-category listed below. Please provide a short explanation of why this PII is shared.

Note: If it is unknown to you whether or not systems share data, you can either contact the business owner of the data or you can contact the IT specialist who knows what other interfaces goes on between the systems / applications.

☐ **Within the DoD Component.**

Specify.

☐ **Other DoD Components**.

Specify.

☐ **Other Federal Agencies**.

Specify.

☐ **State and Local Agencies**.

Specify.

☐ **Contractor** (enter name and describe the language in the contract that safeguards PII)

Specify.

☐ **Other** (e.g., commercial providers, colleges)

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

Note: The opportunity to object is only available at the initial point of data collection. If your system receives PII from a system-to-system interface, the opportunity to object is only available at the source system.

☐ **Yes** ☐ **No**

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

Include the method(s) individuals can use to object to each mode of collection (e.g., telephone, face-to-face, etc.). Include consequences, if any, if an individual objects (i.e., comprehensive healthcare may not be possible).

(2) If "No," state the reason why individuals cannot object.

DoD 5400.11-R, Department of Defense Privacy Program, C4, Disclosures of Personal Information to

Other Agencies and Third Parties, lists the approved circumstances wherein an individual would not be given an opportunity to object to the collection of their PII.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

Note 1: Regarding PHI, authorization must be obtained for uses and disclosures as required and outlined in accordance with DoD 6025.18-R (see references below).

Note 2: Regarding PII only, written consent for specific uses is required in accordance with DoD 5400.11-R (see references below).

☐ **Yes** ☐ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

How is consent obtained from individuals after they provide PII?

If applicable, how is authorization obtained from individuals after they provide PHI?

Does consent require a positive action by an individual rather than being assumed as a default? If so, what is that action?

Would the refusal of an individual to consent to the collection or use of personal information disrupt the level of program service provided to the individual (i.e., comprehensive healthcare may not be possible)? Include the method(s) individuals can use to consent to each specific use (e.g., telephone, face-to-face, etc.) of PII. Include consequences, if any, if an individual withholds consent (i.e., comprehensive healthcare may not be possible).

(2) If "No," state the reason why individuals cannot give or withhold their consent.

DoD 6025.18-R, Chapter 5, Uses and Disclosures For Which An Authorization Is Required, states that a covered entity may not use or disclose PHI without a valid written authorization except as otherwise permitted or required by the Regulation.

Chapter 5 also defines the contents of a valid authorization. No authorization is required for uses and disclosures outlined in Chapter 4, Uses and Disclosures To Carry Out Treatment, Payment, And Healthcare Operations, and Chapter 7, Uses And Disclosures For Which An Authorization Or Opportunity To Agree Or Object Is Not Required.

If PHI is not involved (i.e., only non-health related PII), then DoD 5400.11-R applies, including C4.1.3.2 (requiring written consent by the individual for release outside the DoD of PII from a System of Records) and C4.2 (defining non-consensual conditions of disclosure).

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

Under DoD 5400.11-R, C2.1.4.1, when an individual is requested to furnish PII, a Privacy Act Statement is required, regardless of medium (e.g., telephone, form, personal interview). Please read DoD 5400.11-R, C2.1.4, Privacy Act Statements, for more information.

☐ **Privacy Act Statement** - *If this box is checked, please copy and paste your Privacy Act Statement in the box.*

When an individual is requested to furnish personal information about him or her for inclusion in a system of records, a Privacy Act Statement is required to enable the individual to make an informed decision whether to provide the information requested).

☐ **Privacy Advisory** - *If this box is checked, please copy and paste your Privacy Act Advisory in the box.*

A notification informing an individual as to why information is being solicited and how such information will be used. If PII is solicited by a DoD Web site (e.g., collected as part of an email feedback / comments feature on a Web site) and the information is not maintained in a Privacy Act system of records, the solicitation of such information triggers the requirement for a Privacy Advisory (PA).

☐ **Other**

☐ **None**

Describe each applicable format.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component can restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.

SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply *in the table* below.

☐Name	☐Other Names Used	☐Social Security Number (SSN)
☐Truncated SSN	☐Driver's License	☐Other ID Number
☐Citizenship	☐Legal Status	☐Gender
☐Race/Ethnicity	☐Birth Date	☐Place of Birth
☐Personal Cell Telephone Number	☐Home Telephone Number	☐Personal Email Address
☐Mailing/Home Address	☐Religious Preference	☐Security Clearance
☐Mother's Maiden Name	☐Mother's Middle Name	☐Spouse Information
☐Marital Status	☐Biometrics	☐Child Information
☐Financial Information	☐Medical Information	☐Disability Information
☐Law Enforcement Information	☐Employment Information	☐Military Records
☐Emergency Contact	☐Education Information	☐Other

If "Other," specify *(i.e., passport information, sponsor information, etc.)* or explain any PII grouping selected.

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

Response should indicate all individuals and organizations that provide information to the system from any source, including the individual from whom the information is being collected.

(3) How will the information be collected?

☐ **Paper Form** ☐ **Face-to-Face Contact**
Please indicate all form numbers in the text box for "Other" information.

☐ **Telephone Interview** ☐ **Fax**
Please indicate if a Privacy Act Statement is read to the individual prior to collection.

☐ **Web Site** ☐ **Email**
Please indicate URLs in the text box for "Other" information.

☐ **Information Sharing from System to System**
Please indicate which systems are sharing in the text box for "Other" information.

☐ **Other** - *describe in the text box provided.*

(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?

The following statement provides an acceptable answer to this question because it lists the PII category and gives the reason the PII is being used:

"[System name] may collect name, DOB, and biometrics in order to verify an individual's identity when visiting [your organizations] website."

(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?

Response should indicate how the PII will be used to support the purpose of the system and the underlying mission of the organization.

b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix for data aggregation definition)

Response should indicate:

- ✓ *If the system creates or makes available new or previously unavailable information about an individual; and*
- ✓ *What will be done with the newly identified derived information?*

☐ **Yes** ☐ **No**

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.

Are (or will there be) computer data matching agreement(s) in place which describe who will be responsible for protecting the privacy rights of the beneficiaries and employees affected by the interface between the systems?

c. Who has or will have access to PII in the DoD information system or electronic collection? Indicate all that apply.

Do system administrators provide users access rights based upon job functionality, authority, and responsibility within the enterprise? Response should indicate all individuals who will have access to the system / application, even if the access is only incidental to management, maintenance, troubleshooting, or other support activities.

Is this system covered by a Data Sharing Agreement (DSA)?

- ✓ *If yes, please provide the DUA Number.*

Per role checked below, please describe the level of access.

☐ **Users** ☐ **Developers** ☐ **System Administrators** ☐ **Contractors**

☐ **Other** - *describe in the text box provided.*

d. How will the PII be secured?

(1) Physical Controls *in place or planned*. Indicate all that apply.

- ☐ **Security Guards**
- ☐ **Identification Badges**
- ☐ **Key Cards**
- ☐ **Safes**
- ☐ **Cipher Locks**
- ☐ **Combination Locks**
- ☐ **Closed Circuit Television**
- ☐ **Other** - *describe in the text box provided.*

  - ✓ *Is or will the system be accessed at more than one site? (Provide your answer in the box below.) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?*

(2) Technical Controls *in place or planned*. Indicate all that apply.

- ☐ **User Identification**
- ☐ **Password**
- ☐ **Intrusion Detection System (IDS)**
- ☐ **Encryption** - *describe in the text box provided.*
- ☐ **Biometrics**
- ☐ **Firewall**
- ☐ **Virtual Private Network (VPN)**
- ☐ **DoD Public Key Infrastructure Certificates**

  - ✓ *Is data to/from this system encrypted in transit?*
  - ✓ *Is data at rest encrypted within this system?*

- ☐ **External Certificate Authority (CA) Certificate**
- ☐ **Common Access Card (CAC)**
- ☐ **Other** - *describe in the text box provided.*

  - ✓ *Does/will the system host a web site accessible by the public? (Provide your answer in the box below.)*

(3) Administrative Controls *in place or planned*. Indicate all that apply.

- ☐ **Periodic Security Audits**
- ☐ **Regular Monitoring of Users' Security Practices**
- ☐ **Methods to Ensure Only Authorized Personnel Access to PII**
- ☐ **Encryption of Backups Containing Sensitive Data** – *describe in the text box provided*.

  - ✓ *Please state where backups occur, how often they occur, and how the data is safeguarded. If backups are not encrypted, please provide the DHA PCLO with a POA&M documenting when encryption will occur.*

- ☐ **Backups Secured Off-site**

☐ **Other** - *describe in the text box provided.*

- ✓ *Does this system have a user's manual?*
- ✓ *Are or will there be processes in place for periodic review of PII contained in the system to ensure data integrity, availability, accuracy, and relevancy?*
- ✓ *Does the system maintain audit logs?*

e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?

Please check the appropriate box and enter the date. If you have not received your certification or accreditation, please specify your expected date of completion below, next to the C&A currently being pursued and provide a status of the DIACAP in question g. or h. (whichever applies).

☐ **Yes. Indicate the certification and accreditation status:**

☐ **Authorization to Operate (ATO)** **Date Granted:**

☐ **Interim Authorization to Operate (IATO)** **Date Granted:**

☐ **Denial of Authorization to Operate (DATO)** **Date Granted:**

☐ **Interim Authorization to Test (IATT)** **Date Granted:**

☐ **No**, **this DoD Information system does not require certification and accreditation.**

f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?

According to OMB Circular No. A-130, "the term "information life cycle," means the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition." For the purposes of the PIA, the stages are collection, use, disclosure, processing, retention, and destruction.

Please address each information life cycle phase as listed below:

- ✓ *Collection – Explain how the system collects only the personal information necessary for its purposes. Will steps be taken to ensure that the personal information is accurate, complete, and up-to-date?*
- ✓ *Use and Disclosure – Explain how the system ensures that the sharing of information is to only those identified in the SORN and how PII violations are handled.*
- ✓ *Processing – Explain how data exchange will take place (e.g. over an encrypted network), how component systems and / or applications limit information sharing to those that are functionally necessary.*
- ✓ *Retention and Destruction – Indicate which data retention and destruction schedule(s) are implemented. Explain what and how policies of individual component systems, as stated in their SORNs, govern the retention and disposal of PII collected.*

In addition to providing the information above, please indicate the current system life cycle phase from the following:

1.) Concept Refinement

2.) Technology Development
3.) System Development and Demonstration
4.) Production and Deployment
5.) Operations and Support
6.) Disposal or Decommissioning

g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?

If your information system is a new system, enter N/A and skip to question h.

You must address the following in your answer / risk assessment:

- ✓ *Is all PII evaluated for impact of loss or unauthorized disclosure and protected accordingly?*
- ✓ *Are all electronic PII records assigned a High **or** Moderate impact category and protected at a Confidentiality level of Sensitive **or** higher, unless specifically cleared for public release (Ref. Guide to Protecting the Confidentiality of Personally Identifiable Information" - Special Pub 800-122 or FIPS Pub 199 "Standards for Security Categorization of Federal Information and Information Systems")?*
- ✓ *[If applicable] Are High impact category PII records routinely processed or stored on mobile computing devices or removable electronic media?*
- ✓ *[If applicable] May High impact PII records be accessed by users remotely?*
- ✓ *If PII / PHI may be downloaded to a workstation, mobile computing device, or removable electronic media, what mechanisms are in place to secure that media from unauthorized disclosure, theft, or loss?*
- ✓ *[If applicable] May mobile computing devices that contain High impact PII, including those approved for routine processing, be removed from protected workplaces?*
- ✓ *[If applicable] Does the website employ (or will it employ) persistent tracking technology?*
- ✓ *Are employees or agents with access to personal information in your organization provided with training related to privacy protection?*
- ✓ *Are programs and information technology staff aware of the relevant policies regarding breaches of security or confidentiality?*
- ✓ *Are there controls in place to ensure that data is not made available or disclosed to unauthorized individuals, entities, or processes?*
- ✓ *Are there controls in place to ensure that data has not been altered or destroyed in an unauthorized manner?*

h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?

You must address the following in your answer / risk assessment:

- ✓ *Is all PII evaluated for impact of loss or unauthorized disclosure and protected accordingly?*
- ✓ *Are all electronic PII records assigned a High **or** Moderate impact category and protected at a Confidentiality level of Sensitive **or** higher, unless specifically cleared for public release (Ref. Guide to Protecting the Confidentiality of Personally Identifiable Information" - Special Pub 800-122 or FIPS Pub 199 "Standards for Security Categorization of Federal Information and Information Systems")?*

- ✓ *[If applicable] Are High impact category PII records routinely processed or stored on mobile computing devices or removable electronic media?*
- ✓ *[If applicable] May High impact PII records be accessed by users remotely?*
- ✓ *If PII / PHI may be downloaded to a workstation, mobile computing device, or removable electronic media, what mechanisms are in place to secure that media from unauthorized disclosure, theft, or loss?*
- ✓ *[If applicable] May mobile computing devices that contain High impact PII, including those approved for routine processing, be removed from protected workplaces?*
- ✓ *[If applicable] Does the website employ (or will it employ) persistent tracking technology?*
- ✓ *Are employees or agents with access to personal information in your organization provided with training related to privacy protection?*
- ✓ *Are programs and information technology staff aware of the relevant policies regarding breaches of security or confidentiality?*
- ✓ *Are there controls in place to ensure that data is not made available or disclosed to unauthorized individuals, entities, or processes?*
- ✓ *Are there controls in place to ensure that data has not been altered or destroyed in an unauthorized manner?*

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.

The PIA Team will coordinate the signature process after the PIA has been reviewed and approved by the Chief, DHA PCLO.

Note: If a PIA is not required, only the Program Manager and Program Level Senior Information Assurance Officer need to sign. Please return the signed document to the DHA PCLO.

Program Manager or Designee

Name:

Title:

Organization:

Work Telephone Number:

DSN:

Email Address:

Date of Review:

Other Official Signature (to be used at Component discretion)

Name:

Title:

Organization:

Work Telephone Number:

DSN:

Email Address:

Date of Review:

Other Official Signature (to be used at Component discretion)

Name:

Title:

Organization:

Work Telephone Number:

DSN:

Email Address:

Date of Review:

Component Senior Information Assurance Officer Signature or Designee

Name:

Title:

Organization:

Work Telephone Number:

DSN:

Email Address:

Date of Review:

Component Privacy Officer Signature

Name:

Title:

Work Telephone Number:

DSN:

Email Address:

Date of Review:

Component CIO Signature
(Reviewing Official)

Name:

Title:

Organization:

Work Telephone Number:

DSN:

Email Address:

Date of Review:

Publishing:

Only Sections 1 and 2 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: pia@osd.mil.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Sections 1 and 2.

APPENDIX

Data Aggregation. Any process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to compile information about particular groups based on specific variables such as age, profession, or income.

DoD Information System. A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology (IT)-based processes and platform IT interconnections.

Electronic Collection of Information. Any collection of information enabled by IT.

Federal Personnel. Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits). For the purposes of PIAs, DoD dependents are considered members of the general public.

***Note**: If the system collects data from 10 or more members of the public (see federal personnel definition in the appendix) in a 12 month period, there is a requirement for an OMB Control Number (unless there is an exemption noted in an approved authority).*

Personally Identifiable Information. Information about an individual that identifies, links, relates or is unique to, or describes him or her (e.g., a social security number; age; marital status; race; salary; home telephone number; other demographic, biometric, personnel, medical, and financial information). Also, information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information that is linked or linkable to a specified individual.

Privacy Act Statements. When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, providing a Privacy Act statement is required to enable the individual to make an informed decision whether to provide the information requested.

Privacy Advisory. A notification informing an individual as to why information is being solicited and how such information will be used. If PII is solicited by a DoD Web site (e.g., collected as part of an email feedback/comments feature on a Web site) and the information is not maintained in a Privacy Act system of records, the solicitation of such information triggers the requirement for a privacy advisory (PA).

System of Records Notice (SORN). Public notice of the existence and character of a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be include.